JPA 04-232543 which corresponds to USP-5,414,844

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平4－232543

(43)公開日　平成4年(1992)8月20日

(51)Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
G06F 12/00	537 A	8944-5B		

審査請求　有　　請求項の数5（全 6 頁）

(21)出願番号　特願平3－122192

(22)出願日　平成3年(1991)4月24日

(31)優先権主張番号　528624

(32)優先日　1990年5月24日

(33)優先権主張国　米国（US）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　ダイアナ、エス、ワング
アメリカ合衆国テキサス州、トロフイー、クラブ、クリークモアー、ドライブ、13

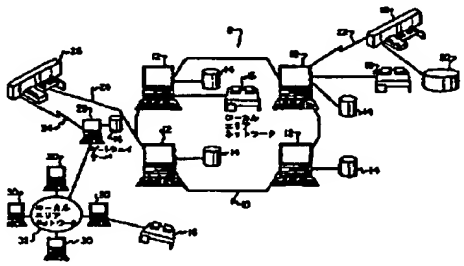
(74)代理人　弁理士　頓宮　孝一　（外５名）

(54)【発明の名称】　データ処理装置内の複数のデータ対象への公的アクセスを制御する方法

(57)【要約】　（修正有）

【目的】　データ処理装置内に記憶された複数のデータ対象に対する公的アクセスの改良された制御方法の提供。

【構成】各アクセス制御プロファイルは各データ対象と関連し、特定のユーザ及びそれに与えられている権限の程度の見出しをリストする明示権限付与パラメタ、複数のユーザ及びリストされた各ユーザに与えられている権限の程度の見出しをリストする共用権限付与パラメタ、及び特定的に述べられていない各ユーザに与えられた権限の程度をリストする公的権限付与パラメタを含んでいる。単独「公的」ユーザ見出しはアクセス制御プロファイル内に特定的に述べていないすべてのユーザに規定し、見出しはデータ対象の全グループのための公的権限付与パラメタとともに単独共有権限付与パラメタ内にリストされ、後に共用権限付与パラメタ内に配置されるので、公的アクセスは単独共有権限付与パラメタにより中央で制御される。



1

【特許請求の範囲】

【請求項1】データ処理装置に記憶された複数のデータ対象への公的アクセスを制御する方法であって、前記データ処理装置は、その中に記憶された各データ対象と関連するアクセス制御プロファイルを有し、前記各アクセス制御プロファイルは、あるユーザおよびそのユーザに与えられた権限の程度の見出しをリストする明示権限付与パラメタ、複数のユーザおよびリストされた各ユーザに与えられた権限の程度の見出しをリストする共有権限付与パラメタ、および前記アクセス制御プロファイルに特定的に識別されていない各ユーザに与えられている権限の程度をリストする公的権限付与パラメタを有し、前記方法は、選択された共有権限付与パラメタ内の複数のデータ対象のすべてに対する公的権限の程度をリストする段階と、前記複数のデータ対象の各々のアクセス制御プロファイル内の前記共有権限付与パラメタを配置する段階と、および前記複数のデータ対象の公的権限の程度が中央で制御される前記複数のデータ対象の各々のアクセス制御プロファイル内の前記公的権限付与パラメタ内の共有権限付与パラメタに対する参照を配置する段階とを有する方法。

【請求項2】請求項1記載の、データ処理装置に記憶された複数のデータ対象への公式アクセスを制御する方法において、選択された共有権限付与パラメタ内の複数のデータ対象のすべてに対する公的権限の程度をリストする段階が、さらに単独ユーザ見出しを前記アクセス制御プロファイル内に特定的に識別されていないユーザのすべてに規定する段階を含む方法。

【請求項3】請求項2記載の、データ処理装置に記憶された複数のデータ対象への公的アクセスを制御する方法において、選択された共有権限付与パラメタ内の複数のデータ対象のすべてに対する公的権限の程度をリストする段階がさらに前記アクセス制御プロファイル内に特定的に識別されていないすべてのユーザに規定されている前記単独ユーザ見出しに対する権限の程度をリストする段階を含む方法。

【請求項4】請求項1記載の、データ処理装置に記憶された複数のデータ対象への公的アクセスを制御する方法であって、さらに、前記複数のデータ対象と関連するアクセス制御プロファイルを記憶する段階を含む方法。

【請求項5】請求項1記載の、データ処理装置に記憶された複数のデータ対象への公的アクセスを制御する方法であって、さらに、前記アクセス制御プロファイル内の前記複数のデータ対象の各々の所見者の見出しを記憶する段階を含む方法。

【発明の詳細な説明】

【0001】〔発明の背景〕1　技術分野

本発明は、一般的に、データ処理装置の改良に関し、特にデータ処理装置内に記憶された複数のデータ対象への公的アクセスの制御方法に関する。さらに特別に、本発明は、データ処理装置内に記憶された複数のデータ対象への公的アクセスの中央制御方法に関する。

2

【0002】2　関連技術の説明

現代のデータ処理装置において、装置内の各種の資料およびアプリケーションへのアクセスの制御は、よく知られている。高度に制御された機密保護装置においては、特定のユーザが、実際にそのデータ対象にアクセスする権限のあるユーザであることを証明する各種の手順の後にのみ可能である。

【0003】さらに複雑なデータ処理装置においては、アクセスの制御は特定のユーザばかりでなく、そのユーザのもっている権限の程度までも選択識別することによってさらに規定される。例えば、あるユーザは、選択されたデータ対象を読み出すことはできるが、そのデータ対象を変更することはできない。同様に、あるユーザは、データを選択されたデータ対象に書き込む権限をもっているが、そのデータ対象の他の部分を読み出すことは許されていない。勿論、権限の程度の各種の他の組合せがそのような装置で履行されることを当該技術に習熟している人たちは理解している。

【0004】データ処理装置に記憶された各種のデータ対象に対するＩＢＭの文書交換アーキテクチャ・アクセス制御は、アクセス制御・モデル・オブジェクト（ＡＣＭＯ）という名で知られているアクセス制御プロファイルによって制御されている。ＡＣＭＯは、関連資料に関するアクセス制御情報のリポジットリを提供し、資料の所有者の見出し、アクセス権限のある形式が与えられているユーザの見出し、資料が装置内に保持されていなければならい期間、およびその資料に機密保持の程度が含まれている。

【0005】選択された資料のアクセス制御は、数個の権限付与パラメタの一つを利用するＡＣＭＯ内に規定されている。明示権限付与パラメタは、特定のユーザおよびそのユーザの権限の程度の特定の見出しをリストにするために利用される。共用権限パラメタは、データ対象のグループに対する、多数のユーザおよび各ユーザの権限の程度の見出しを含んだ共用権限リストの見出しをリストにするために利用される。最後に、公的権限付与パラメタは、ＡＣＭＯ内に、特定的に述べられていないユーザの権限の程度を設定するために利用される。

【0006】前述の装置は、データ処理装置内に記憶された選択されたデータ対象へのアクセスを制御する優れた方法を提供するが、データ対象のグループに対する特定化されていないか、または、「公的」なアクセスを効果的に制御する方法を提供できない。例えば、ユーザが同一の権限の程度で、多数のデータ対象について公的アクセスをあたえられることを望むこともありうる。現在のアーキテクチャでは、ユーザは各データ対象に個々にアクセスし、その後、各データ対象内の公的権限付与パラメタの内容を変更しなければならない。従って、複数

3

のデータ対象に対する公的アクセスを中央で制御できる方法が必要であることは明かである。

【０００７】〔発明の要約〕従って、本発明の一つの目的は、データ処理装置管理の改良された方法を提供することである。

【０００８】また、本発明の他の目的は、データ処理装置内に記憶された複数のデータ対象に対する公的アクセスの改良された制御方法を提供することである。

【０００９】さらに、本発明の他の目的は、データ処理装置内に記憶された複数のデータ対象の公的アクセスを中央で制御する改良された方法を提供することである。

【００１０】上述の目的は、以下に説明する方法で達成される。アクセス制御プロファイルは、データ処理装置内に記憶された各データ対象と結合される。各アクセス制御プロファイルは、前もって、特定のユーザおよびそのユーザに与えられている権限の程度の見出しをリストにする明示権限付与パラメタ、複数のユーザおよびリストされている各ユーザに与えられている権限の程度の見出しをリストにする共用権限付与パラメタ、およびアクセス制御プロファイル内に特定的に述べられていない各ユーザに与えられている権限の程度をリストにする公的権限付与パラメタを含んでいる。単独の「公的」ユーザの見出しは、次いでアクセス制御プロファイル内に特定的に述べられていないすべてのユーザに対して規定され、その見出しは、データ対象の全グループの公的権限の程度とともに、単独の共用権限付与パラメタ内にリストされる。その共用権限付与パラメタは、次ぎにグループ内の各データ対象のアクセス制御プロファイル内に配置される。その後、共用権限付与パラメタに対する参照が、グループ内の各データ対象の公的権限付与パラメタ内に配置されるので、データ対象の全グループに対する公的アクセスは、単独共用権限付与パラメタによって中央で制御される。

【００１１】〔実施例〕図、特に図１では、本発明の方法を実施するために利用できるデータ処理装置を図解的に表現している。図に示されているように、データ処理装置８には、ローカル・エリア・ネットワーク（ＬＡＮ）１０および３２などの複数のネットワークがあり、その各々にはそれぞれ複数の独立したコンピュータ１２および３０があることが好ましい。勿論、当該技術に習熟した人たちは、ホスト処理装置と結合した複数のインテリジェント・ワーク・ステーション（ＩＷＳ）が、そのようなネットワークの各々に利用できることを理解している。

【００１２】そのようなデータ処理装置に共通なように、個々のコンピュータは、記憶装置１４および（または）プリンタ／出力装置１６と結合している。一つ以上の記憶装置１４が、本発明の方法に従って利用され、周期的にアクセスされ、データ処理装置８内でユーザに処理される各種のデータ対象または資料が記憶される。従

4

来の技術でよく知られている方法で、各データ処理手順または資料が、資源管理またはライブラリ・サービスと結合した記憶装置１４に記憶される。ライブラリ・サービスは、結合している資源対象のすべてを保持および更新することができる。

【００１３】さらに、図１を参照すれば、データ処理ネットワーク８には、また、通信リンク２２によって、ローカル・エリア・ネットワーク（ＬＡＮ）１０に結合されているメインフレーム・コンピュータ１８などの多数のメインフレーム・コンピュータがある。メインフレーム１８はローカル・エリア・ネットワーク（ＬＡＮ）１０用の遠隔記憶として働く記憶装置２０と結合している。ＬＡＮ１０は通信制御装置２７および通信リンク３４を介してゲートウェイ・サーバ２８に結合している。ゲートウェイ・サーバ２８は、独立のコンピュータまたは、ローカル・エリア・ネットワーク（ＬＡＮ）３２をローカル・エリア・ネットワーク（ＬＡＮ）１０にリンクするインテリジェント・ワーク・ステーションであることが望ましい。

【００１４】ローカル・エリア・ネットワーク（ＬＡＮ）３２およびローカル・エリア・ネットワーク（ＬＡＮ）１０について論じたように、複数のデータ処理手順または資料は記憶装置２０に記憶され、このように記憶されたデータ処理手順および資料用の資源管理またはライブラリ・サービスとしてのメインフレーム・コンピュータ１８によって制御される。勿論、当該技術に習熟した人たちは、メインフレーム・コンピュータ１８がローカル・エリア・ネットワーク（ＬＡＮ）１０から、幾何学的に遠距離にあること、また同様に、ローカル・エリア・ネットワーク（ＬＡＮ）１０が、ローカル・エリア・ネットワーク（ＬＡＮ）３２から相当な距離のところにあることを理解している。すなわち、ローカル・エリア・ネット・ワーク（ＬＡＮ）３２は、カリフォルニアにあり、ローカル・エリア・ネト・ワーク（ＬＡＮ）１０はテキサスにあり、そしてメインフレーム・コンピュータ１８はニューヨークにあってもよい。

【００１５】前述のことから理解されるように、配置されたデータ処理ネットワーク８の一部分内のユーザが、データ処理ネットワーク８の他の部分に記憶されているデータ対象または資料にアクセスすることの望まれることが、しばしばある。データ処理ネットワーク８に記憶された資料内のセンブランス・オブ・オーダを保持するために、アクセス制御プログラムを作ることが望ましいことがしばしばある。上述のように、これは一般に各ユーザがある資料について持っている権限の程度とともに、個々のデータ対象または資料に対するアクセス権をもっている人たちをリストすることによって達成される。また、多数のデータ対象または資料と関連したアクセス制御プロファイル内に記憶された共用権限付与パラメタ内のユーザおよび権限の程度を識別することによっ

て、ユーザのあるグループに、特定の資料にアクセスすることを許可するか、または、リストされているあるユーザに、資料のグループにアクセスすることを許可することは、よく知られている。

【００１６】しかし、当業者たちが理解しているように、アクセス制御プロファイルでアクセス権をあらかじめ与えられていないユーザの場合にも、そのユーザに特定の資料にアクセスすることを許可する必要があるか、または許可することが望ましいことがしばしばある。このいわゆる「公的」アクセスは、一般的に既存の機密保持の水準で多数の個人によるアクセスが認められるような資料に関して、選択された権限の程度で許可される。これは一般に従来の技術において、アクセス制御プロファイル内の公的権限付与の程度を設立することによって達成される。アクセス制御プロファイルは、アクセス制御プロファイル内に、特定的に述べられていないなどの個々のユーザに対しても権限の程度を設定する。

【００１７】当業者たちは、多数の資料グループに対して権限の程度を設立することは、従来の技術では、個々の各データ対象にアクセスし、その後、そのデータ対象に対する公的権限付与パラメタの内容を変更することによってのみ達成できることを理解している。本発明の方法では、多数のデータ対象のグループに対する公的アクセスが中央制御されるような方法で設定する。

【００１８】図２を参照すれば、本発明の方法に従ったデータ対象およびそれと結合したアクセス制御プロファイルが図解的に表現されている。図からわかるように、データ対象４０が示されている。データ対象４０には、ライブラリ・オブジェクト４２およびアクセス制御モデル・オブジェクト（ＡＣＭＯ）４４が含まれている。ＡＣＭＯ４４内には、ライブラリ・オブジェクト４２を所有するユーザの名前を設定するオーナ見出し４６がリストされている。さらに、明示権限付与パラメタ４８がリストされており、従来の技術による既知の方法で、特定の個々のユーザおよびライブラリ・オブジェクト４２に関してもっている権限の程度の見出しを設定するために利用される。

【００１９】また、ＡＣＭＯ４４内には、多数のユーザおよびそのユーザたちが、共用権限付与パラメタ５０を利用する複数のライブラリ・オブジェクトすべてに関してもっている権限の程度の見出しを設定する共用権限付与パラメタ５０がリストされている。最後に、ＡＣＭＯ４４には、公的権限付与パラメタ５２がリストされており、これは明示権限付与パラメタ４８または共用権限付与パラメタ５０内に特定的に述べられていないユーザに許可される権限の程度を設定するために利用される。本発明の重要な特徴によれば、公的権限付与パラメタ５２は、ライブラリ・オブジェクト４２の公的ユーザに許可される権限の程度を設定するほかにも利用できる。

【００２０】図で説明されているように、公的権限付与パラメタ５２は共用権限付与パラメタ５０に対する参照を含んでいる。共用権限付与パラメタ５０は、参照数字５４で非常に詳細に設定されており、ユーザ見出し５６の欄および欄５８に述べられた各ユーザに対する関連権限の程度を含んでいる。図で説明されているように、ユーザＡは、ライブラリ・オブジェクト４２およびその関連のＡＣＭＯ内に共有権限付与パラメタ５０を含んでいる他のライブラリ・オブジェクトを読み出す権限をもっている。

【００２１】同様に、ユーザＢは、ライブラリ・オブジェクト４２およびその関連のＡＣＭＯ内に共用権限付与パラメタ５０を含んでいる他のライブラリ・オブジェクトに書き込む権限をもっている。また同様に、ユーザＣは、ライブラリ・オブジェクト４２および共用権限付与パラメタ５０を含んでいる他のライブラリ・オブジェクトに関して、制限のない権限を許可されている。

【００２２】最後に、本発明の方法に従って、ユーザ見出し「公的」は、共用権限付与パラメタ５０の欄５６に設定され、関連の権限の程度は共用権限付与パラメタ５０の欄５８にリストされる。当業者たちは、以上を参照して、ある単独のユーザ見出しを、ＡＣＭＯ５０内に特定的に述べられていないすべてのユーザに規定し、また、ある権限の程度を共用権限付与パラメタ５０内のすべてのユーザに設定することによって、ライブラリ・オブジェクト４２および共用権限付与パラメタ５０を含む他のすべてのライブラリ・オブジェクトに対する公的アクセスが簡単になり、各ライブラリ・オブジェクトの公的権限付与パラメタ内の共用権限付与パラメタ５０に対する参照を挿入することによって効果的に制御できることを理解するであろう。

【００２３】図３には、本発明の方法に従って、複数のデータ対象に対するアクセス制御の確立を説明する高水準のフローチャートが示されている。図で説明されているように、プロセスはブロック６０で始まり、その後ユーザがある資料グループに対して公的権限の程度を設定するブロック６２を通る。次に、プロセスは、その資料グループに含まれる資料の指定を説明するブロック６４を通る。その後、ユーザによって設定された公的ユーザ権限の程度が、図２で表された方法で、共用権限付与パラメタ内にリストされる。

【００２４】次にブロック６８で説明されているように、資料グループ内の各資料について次のステップが行われる。まず、ブロック７０は、資料グループ内の各資料用のアクセス制御モデル・オブジェクト（ＡＣＭＯ）内の望みの公的権限の程度を含む共用権限付与パラメタの位置を明示する。その後、共用権限付与パラメタに対する参照が、グループ内の各資料のＡＣＭＯ内の公的権限付与パラメタ内に位置決めされる。ＡＣＭＯ内に特定的に述べられていないユーザによる企画されたアクセスは、資料のグループの各資料の公的権限の程度を設定す

る単独の共用権限付与パラメタに対する参照となる。ブロック７４は処理されている資料が、グループの最後の資料かどうかを決定し、最後でなければ、プロセスはブロック６８に戻り、反復式に進行する。その時、現在処理されている資料が、指定の資料グループの最後の資料であれば、ブロック７６に示されているようにプロセスは終了する。第４図には、本発明の方法に従って、データ対象のアクセスを図示する高水準のフローチャートが画かれている。図で示されているように、プロセスはブロック８０で始まり、その後、資料またはデータ対象のアクセスが要求されているかどうかの決定を示すブロック８２を通る。要求されていなければ、プロセスはアクセスが要求されるまで、単に反復する。

【００２５】ブロック８２で決定されて特定の資料が要求されていると、ブロック８４はアクセスを要求しているユーザが、リストされているユーザかどうかの決定を示す。「リストされているユーザ」の意味しているものは、そのユーザの見出しが、問題の資料に対するＡＣＭＯ内に特定的に設定されているということである。ブロック８４で決定されて、その資料に対してアクセスを要求しているユーザが、リストされているユーザである場合は、ブロック８６は問題のユーザが望みのアクションに対して十分な権限を持っているかどうかの決定を示す。権限を持っていない場合は、エラー・メッセジが、ブロック８８のように示される。問題のユーザが望みのアクションに対し十分な権限を持っている場合は、ブロック９０に表されているように、アクセスが許可される。

【００２６】再びブロック８４を参照して、特定の資料へのアクセスを要求しているユーザがＡＣＭＯ内に特定的に述べられたリストされたユーザでない場合は、ブロック９２が、特定の公的権限程度が問題のデータ対象に対する公的権限付与パラメタ内に設定されているかどうかの決定を示す。設定されていれば、プロセスはブロック８６に行き、問題の公的ユーザが、望みのアクションに対して十分な権限をもっているかどうかを決定する。上述のごとく、公的ユーザの権限の程度によって、アクセスが許可されるか、またはエラーメッセージが示される。

【００２７】再びブロック９２を参照して、特定の公的権限程度が、問題の資料に対するＡＣＭＯの公的権限付与パラメタ内にリストされていない場合は、ブロック９

４が、共用権限付与パラメタ内に対する参照を含んでいるかどうかの決定を示す。含んでいない場合は、システムはエラーメッセージを示して、アクセスは拒否される。しかし、公的権限付与パラメタが、共有権限付与パラメタに対する参照を含んでいる場合には、ブロック９６が、上述のごとく、共有権限付与パラメタ内に設定されたパラメタに従って確立された公的ユーザの権限程度の決定を示す。

【００２８】共用権限付与パラメタから公的権限の程度を決めた後、プロセスは再び公的権限の程度が、ユーザが望んでいるアクションに対して十分なものであるかどうかを決めるブロック８６に戻る。その後、その決定に従って、アクセスが拒否されるか、または許可される。

【００２９】上述を参照して、当該技術に習熟した人たちは、本発明の出願者が多数のデータ対象へのアクセスをある特定の資料に対するアクセス制御プロファイル内に特定的に述べられていないすべてのユーザのユーザ見出しを規定すること、および多数のデータ対象のアクセス制御プロファイル内に位置が決められている単独共用権限付与パラメタ内のユーザ見出しに対する権限の程度を設定することによって、中央で制御する方法を説明したことを理解できるであろう。各資料中の公的権限付与パラメタ内の共用権限付与パラメタに対する参照を単に含むことによって、多数の資料に関する公的ユーザの権限の程度が簡単にしかも効率的に、単独の場所に設定される。

【図面の簡単な説明】

【図１】本発明の方法を実施するために利用できる分割したデータ処理装置を図解的に表現した図。

【図２】本発明の方法に従って、データ対象およびその関連のアクセス制御プロファイルを図解的に表現した図。

【図３】本発明の方法に従って、複数のデータ対象のアクセス制御の確立を示す高水準のフローチャート。

【図４】本発明の方法に従った、データ対象のアクセスを示す高水準のフローチャート。

【符号の説明】

８　データ処理装置

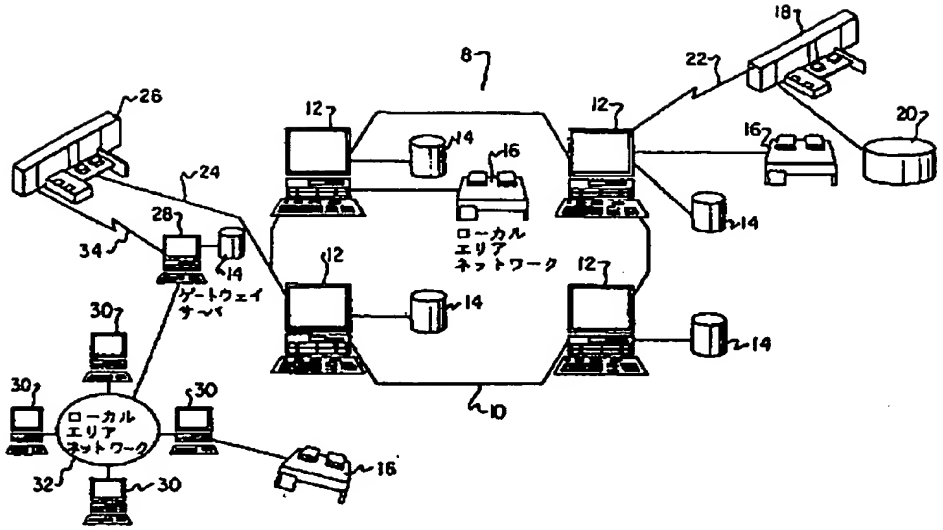
１０，３２　ローカルエリア・ネットワーク

１２，３０　独立したコンピュータ

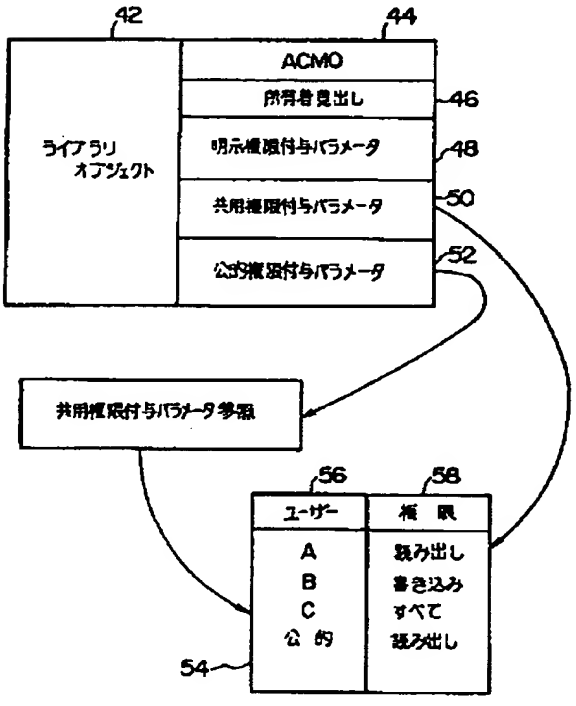
１４　記憶装置

１６　プリンタ／出力装置

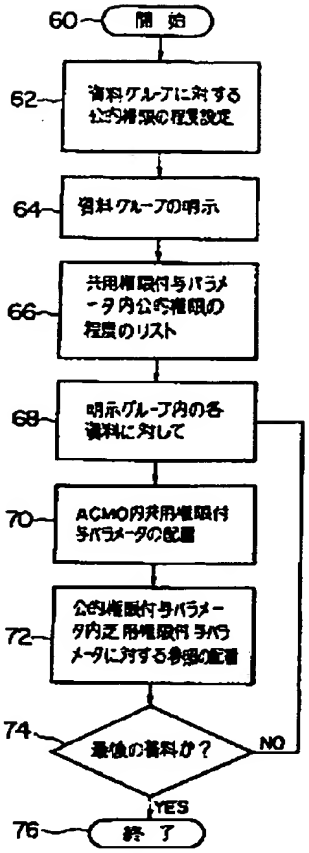
【図1】


ローカル
エリア
ネットワーク
ゲートウェイ
サーバ
ローカル
エリア
ネットワーク

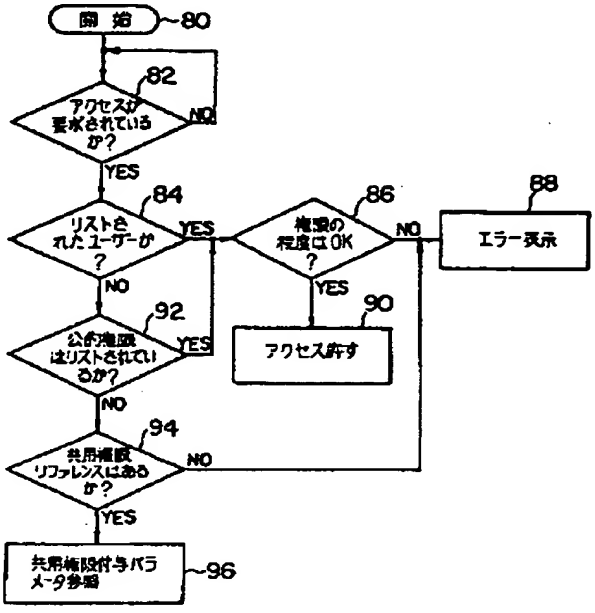
【図2】


ライブラリ
オブジェクト
ACMO
所有者見出し
明示権限付与パラメータ
共用権限付与パラメータ
公的権限付与パラメータ
共用権限付与パラメータ参照
ユーザー
権限
A
B
C
公的
読み出し
書き込み
すべて
読み出し

【図3】


開始
資料グループに対する公的権限の程度設定
資料グループの明示
共用権限付与パラメータ内公的権限の程度のリスト
明示グループ内の各資料に対して
ACMO内共用権限付与パラメータの配置
公的権限付与パラメータ内の共用権限付与パラメータに対する参照の配置
最後の資料か？
NO
YES
終了

【図4】


開始
アクセスが要求されているか？
NO
YES
リストされたユーザーか？
YES
NO
権限の程度はOK？
NO
YES
エラー表示
アクセス許す
公的権限はリストされているか？
YES
NO
共用権限リファレンスにあるか？
NO
YES
共用権限付与パラメータ参照